Team Name: sdmay24-29

Team Members: Daniel Ocampo, Trent Bickford, Ella Cook, Westin Chamberlain
Report Period: October 8 – October 22

Summary of Progress in this Period

Progress Point	**Notes**
Delved into the inner workings of the virtual machines handling the PowerCyber infrastructure.	• In our latest meeting with our adviser we had a walkthrough of the Siemens-based virtual machines that were set up to control the PowerCyber industrial control systems framework. • Better understanding of the specific types of nodes (manager, etc) that we plan to implement within SecurityOnion on the PowerCyber setup. • The overall architecture of the system is complex. It will be necessary to break it down and ask for diagrams. To understand what it means in greater detail.
Got access to the rest of the virtual machines on vSphere.	• Now that we can access resources in vSphere. Our team will make use of them to set up our commercial and open source SIEM solution, Gravwell and SecurityOnion respectively.
Suporting software resources presentation.	• On Oct. 10th our team had the opportunity to present to our adviser some of the software resources that could provide helpful functionality to our project. Some of these tools include Kibana, CyberChef, navigator and a playbook handler. • These will be very helpful when handling incidents manually and provide the capability to automate some of the work.

Gravwell presentation.	• While the project is based on SecurityOnion. Our project adviser is encouraging us to explore SIEM alternatives that are promising. One of the platforms we are looking at is Gravwell which is a commercially available data processing solution whose creators attempt to address everything that their competitor Splunk seems to lack. • Our team believes that Gravwell is a very flexible and simple to use option that can help us build playbooks to automate a lot of the manual incident work. Automated scripts can also be created to conduct custom processes. The good thing about Gravwell is that it is able to integrate well with other data parsing tools, so we do not lose any existing capabilities by embracing Gravwell instead of SecurityOnion. It can get expensive so this might not be a viable option.
Project Design Lightning Talk	• Our lighting talk this week will be based on project design, this will be the most content heavy lightning talk to date. Since our future work in the spring semester will depend heavily on design. • In the presentation we covered sections such as project design complexity, engineering tools used, design context, design decisions, functionality and technology considerations.

Pending Issues

Issue	Description
Continue to make use of free online training resources to become comfortable using SecurityOnion and Gravwell.	• Since our team will be granted access to virtual resources soon. We need to be able to have a good understanding of how to start configuring and making sense of all the capabilities provided by security onion. We do this by searching for training videos and resources available for free on the internet. • Now that a virtual machine has been set up in Vsphere for us to use with Gravwell we need to go through the documentation and set it up properly.
Waiting for diagrams covering PowerCyber from project adviser.	• After our weekly adviser meeting, we need new resources to move on to our next step. This week we need diagrams which help describe the PowerCyber architecture.
Integration of machine learning into project.	• For an analyst to do the incident handling portion of the project would be overwhelming. Which is why we have a SIEM to help collect and parse the noise from the real threats. The next step above that is to train a machine learning model to detect a new previously unknown threat based on prior threat signatures.
Schedule a Demo with a Gravwell representative.	• In an effort to better understand how we could set up our Gravwell implementation on a virtual machine. We need to set up a time to talk with a Gravwell representative. For a breakdown on the installation.

Plans for Upcoming Reporting Period

Pending Item	Notes
Integrate MITRE Caldera into project to deploy attacks on OT systems.	• Since this is one of the portions of the project that will be implemented last, it follows that we have not done enough research to thoroughly understand how testing with MITRE Caldera will be accomplished. • We will use the newly available Kali linux virtual machines for this
Develop weekly slide deck to showcase progress to our project adviser. Stay prepared for in-class lightning talks.	• In order to be prepared to present during the in-class lighting talks our group needs to develop a new slide deck covering project planning. • As well as a secondary slide deck to showcase new findings to our project adviser.
Design Implementation.	• By the time reporting period 4 comes around our group would have taken our first steps into the realm of design implementation.
Documentation	• Set up templates for documentation of project processes.